

**Data communications encryption synchronisation for cellular radio - has rapid resynchronisation of mobile station with new base station upon hand-off and ensures resynchronisation upon failure**

Patent Assignee: ERICSSON GE MOBILE COMMUNICATIONS (TELF); ERICSSON GE MOBILE COMMUNICATIONS INC (TELF); ERICSSON INC (TELF)

Inventor: DENT P; DENT P W

Patent Family ( 12 patents, 8 countries )

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
US 5081679	A	19920114	US 1990556103	A	19900720	199206	B
WO 1992002088	A	19920206	WO 1991US5086	A	19910718	199208	E
AU 199186267	A	19920218	AU 199186267	A	19910718	199222	E
			WO 1991US5086	A	19910718		
CN 1058499	A	19920205	CN 1991105012	A	19910720	199241	E
GB 2261349	A	19930512	WO 1991US5086	A	19910718	199319	E
			GB 199226465	A	19921218		
JP 6501139	W	19940203	JP 1991516019	A	19910718	199410	E
			WO 1991US5086	A	19910718		
AU 648960	B	19940505	AU 199186267	A	19910718	199423	E
NZ 238652	A	19940325	NZ 238652	A	19910621	199426	E
GB 2261349	B	19941019	WO 1991US5086	A	19910718	199439	E
			GB 199226465	A	19921218		
CA 2087615	C	19990202	CA 2087615	A	19910718	199916	E
KR 123945	B1	19971201	WO 1991US5086	A	19910718	199951	E
			KR 1993700103	A	19930115		
CN 1039762	C	19980909	CN 1991105012	A	19910720	200457	E

Priority Applications (no., kind, date): US 1990556103 A 19900720

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
WO 1992002088	A	EN				
National Designated States,Original	AU CA GB JP KR					
AU 199186267	A	EN			PCT Application	WO 1991US5086
					Based on OPI patent	WO 1992002088
GB 2261349	A	EN			PCT Application	WO 1991US5086
					Based on OPI patent	WO 1992002088
JP 6501139	W	JA			PCT Application	WO 1991US5086
					Based on OPI patent	WO 1992002088
AU 648960	B	EN			Previously issued patent	AU 9186267
					Based on OPI patent	WO 1992002088
NZ 238652	A	EN				
GB 2261349	B	EN			PCT Application	WO 1991US5086
					Based on OPI patent	WO 1992002088

CA 2087615	C	EN			PCT Application	WO 1991US5086
KR 123945	B1	KO				

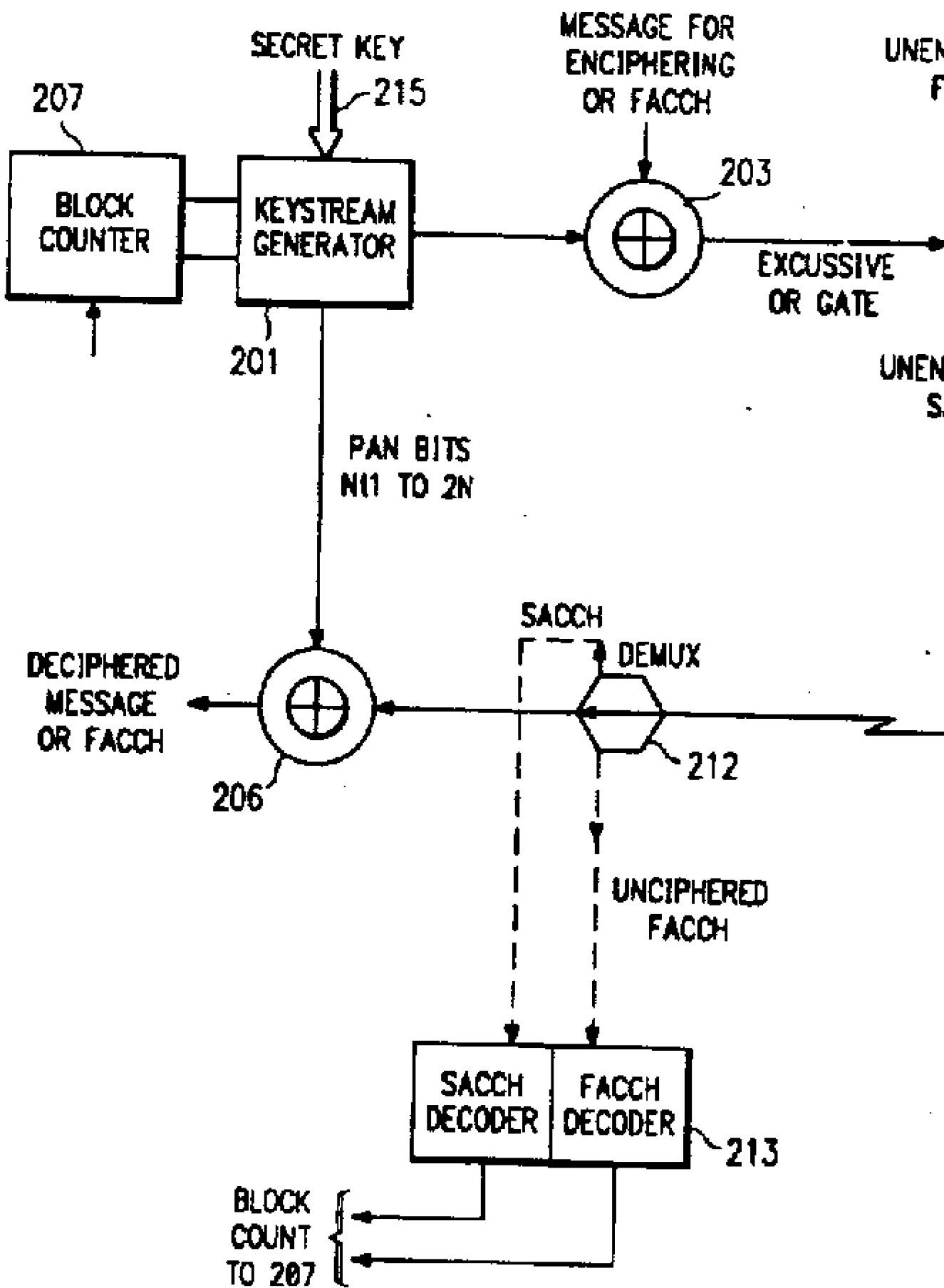
### **Alerting Abstract US A**

The system for the synchronisation of encryption and decryption in a duplex cellular radio system switches an encrypted call from one cell to another. At the instant of handoff, a rapid first resynchronisation device temporarily seizes the voice channel in one direction only and transmits synchronisation information in such one direction. The first resynchronisation device ceases to transmit the synchronisation information and releases such one direction of the voice channel as soon as an indicator of successful resynchronisation is detected in the other direction. Transmission of speech traffic in such one direction is then resumed after such detection of successful resynchronisation.

An upper limit is set on the length of time which the first rapid synchronisation device may cease such one direction. After such timeout, resynchronisation information may be provided by a second resynchronisation device at a slower rate through a slow rate control channel bit stream which is multiplexed with the traffic data.

**ADVANTAGE** - Avoid occupying one direction with continuous transmission of synchronisation information in event successful resynchronisation has occurred but has not been detected due to faulty transmission in othe direction. @/(16pp Dwg.No.4/4)@

### **Main Drawing Sheet(s) or Clipped Structure(s)**



**Title Terms /Index Terms/Additional Words:** DATA; COMMUNICATE; ENCRYPTION; SYNCHRONISATION; CELLULAR; RADIO; RAPID; RESYNCHRONISATION; MOBILE; STATION ; NEW; BASE; HAND; ENSURE; FAIL

### Class Codes

International Patent Classification

IPC	Class Level	Scope	Position	Status	Version Date
H04Q-007/04			Main		"Version 7"
H04B-007/26; H04L-009/10			Secondary		"Version 7"
H04L-0009/00	A	I	L	R	20060101
H04L-0009/12	A	I		R	20060101
H04W-0012/00	A	I		R	20090101
H04L-0009/00	C	I	L	R	20060101
H04L-0009/12	C	I		R	20060101
H04W-0012/00	C	I		R	20090101

**ECLA:** H04L-009/12, H04Q-007/38S, H04W-012/02

**ICO:** T04Q-007:38H

**US Classification, Current** Main: 380-272000; Secondary: 380-043000, 380-260000, 380-274000, 455-438000

**US Classification, Issued:** 38048, 37959, 37960, 38043, 38049, 45533.2

File Segment: EPI;

DWPI Class: W01; W02

Manual Codes (EPI/S-X): W01-A04; W01-A05A; W01-B05A1A; W02-C03C1A

### Original Publication Data by Authority

### Australia

**Publication No.** AU 648960 B (Update 199423 E)

Publication Date: 19940505

Assignee: ERICSSON GE MOBILE COMMUNICATIONS (TELF)

Inventor: DENT P W

Language: EN

Application: AU 199186267 A 19910718 (Local application)

Priority: US 1990556103 A 19900720

Related Publication: AU 9186267 A (Previously issued patent)

WO 1992002088 A (Based on OPI patent )

Original IPC: H04L-7/00(A) H04L-9/00(B)

Current IPC: H04L-9/00(R,A,I,M,JP,20060101,20051220,A,L) H04L-

9/00(R,I,M,JP,20060101,20051220,C,L) H04L-9/12(R,I,M,EP,20060101,20051008,A) H04L-

9/12(R,I,M,EP,20060101,20051008,C) H04W-12/00(R,I,M,EP,20090101,20090105,A) H04W-

12/00(R,I,M,EP,20090101,20090105,C)  
Current ECLA class: H04L-9/12 H04Q-7/38S H04W-12/02  
Current ECLA ICO class: T04Q-7:38H

**Publication No.** AU 199186267 A (Update 199222 E)

Publication Date: 19920218

Assignee: ERICSSON GE MOBILE COMMUNICATIONS (TELF)  
ERICSSON GE MOBILE COMMUNICATIONS (TELF)

Inventor: DENT P W

Language: EN

Application: AU 199186267 A 19910718 (Local application)  
WO 1991US5086 A 19910718 (PCT Application)

Priority: US 1990556103 A 19900720

Related Publication: WO 1992002088 A (Based on OPI patent )

Original IPC: H04L-9/00(A)

Current IPC: H04L-9/00(R,A,I,M,JP,20060101,20051220,A,L) H04L-  
9/00(R,I,M,JP,20060101,20051220,C,L) H04L-9/12(R,I,M,EP,20060101,20051008,A) H04L-  
9/12(R,I,M,EP,20060101,20051008,C) H04W-12/00(R,I,M,EP,20090101,20090105,A) H04W-  
12/00(R,I,M,EP,20090101,20090105,C)

Current ECLA class: H04L-9/12 H04Q-7/38S H04W-12/02

Current ECLA ICO class: T04Q-7:38H

## Canada

**Publication No.** CA 2087615 C (Update 199916 E)

Publication Date: 19990202

Assignee: ERICSSON INC (TELF)

Inventor: DENT P W

Language: EN

Application: CA 2087615 A 19910718 (Local application)

Priority: US 1990556103 A 19900720

Original IPC: H04L-9/14(A) H04Q-7/22(B) H04Q-7/38(B)

Current IPC: H04L-9/00(R,A,I,M,JP,20060101,20051220,A,L) H04L-  
9/00(R,I,M,JP,20060101,20051220,C,L) H04L-9/12(R,I,M,EP,20060101,20051008,A) H04L-  
9/12(R,I,M,EP,20060101,20051008,C) H04W-12/00(R,I,M,EP,20090101,20090105,A) H04W-  
12/00(R,I,M,EP,20090101,20090105,C)

Current ECLA class: H04L-9/12 H04Q-7/38S H04W-12/02

Current ECLA ICO class: T04Q-7:38H

## China

**Publication No.** CN 1039762 C (Update 200457 E)

Publication Date: 19980909

Assignee: ERICSSON GE MOBILE COMMUNICATIONS INC; US (TELF)

Language: ZH

Application: CN 1991105012 A 19910720 (Local application)

Priority: US 1990556103 A 19900720

Original IPC: H04L-7/04(A)  
Current IPC: H04L-9/00(R,A,I,M,JP,20060101,20051220,A,L) H04L-9/00(R,I,M,JP,20060101,20051220,C,L) H04L-9/12(R,I,M,EP,20060101,20051008,A) H04L-9/12(R,I,M,EP,20060101,20051008,C) H04W-12/00(R,I,M,EP,20090101,20090105,A) H04W-12/00(R,I,M,EP,20090101,20090105,C)  
Current ECLA class: H04L-9/12 H04Q-7/38S H04W-12/02  
Current ECLA ICO class: T04Q-7:38H

**Publication No.** CN 1058499 A (Update 199241 E)

Publication Date: 19920205

Assignee: ERICSSON GE MOBILE COMMUNICATIONS; US (TELF)

Inventor: DENT P

Language: ZH

Application: CN 1991105012 A 19910720 (Local application)

Priority: US 1990556103 A 19900720

Original IPC: H04B-7/26(A) H04L-7/04(B) H04Q-7/00(B)

Current IPC: H04L-9/00(R,A,I,M,JP,20060101,20051220,A,L) H04L-9/00(R,I,M,JP,20060101,20051220,C,L) H04L-9/12(R,I,M,EP,20060101,20051008,A) H04L-9/12(R,I,M,EP,20060101,20060101,C) H04W-12/00(R,I,M,EP,20090101,20090105,A) H04W-12/00(R,I,M,EP,20090101,20090105,C)

Current ECLA class: H04L-9/12 H04Q-7/38S H04W-12/02

Current ECLA ICO class: T04Q-7:38H

## Great Britain

**Publication No.** GB 2261349 A (Update 199319 E)

Publication Date: 19930512

Assignee: ERICSSON GE MOBILE COMMUNICATIONS (TELF)

Language: EN

Application: WO 1991US5086 A 19910718 (PCT Application)

GB 199226465 A 19921218 (Local application)

Priority: US 1990556103 A 19900720

Related Publication: WO 1992002088 A (Based on OPI patent )

Original IPC: H04L-9/12(A)

Current IPC: H04L-9/00(R,A,I,M,JP,20060101,20051220,A,L) H04L-9/00(R,I,M,JP,20060101,20051220,C,L) H04L-9/12(R,I,M,EP,20060101,20051008,A) H04L-9/12(R,I,M,EP,20060101,20051008,C) H04W-12/00(R,I,M,EP,20090101,20090105,A) H04W-12/00(R,I,M,EP,20090101,20090105,C)

Current ECLA class: H04L-9/12 H04Q-7/38S H04W-12/02

Current ECLA ICO class: T04Q-7:38H

Claim: The system for the synchronisation of encryption and decryption in a duplex cellular radio system switches an encrypted call from one cell to another. At the instant of handoff, a rapid first resynchronisation device temporarily seizes the voice channel in one direction only and transmits synchronisation information in such one direction. The first resynchronisation device ceases to transmit the synchronisation information and releases such one direction of the voice channel as soon as an indicator of successful resynchronisation is detected in the other direction. Transmission of speech traffic in such one direction is then resumed after such detection of successful resynchronisation.

An upper limit is set on the length of time which the first rapid synchronisation device may cease such one direction. After such timeout, resynchronisation information may be provided by a second resynchronisation device at a slower rate through a slow rate control channel bit stream which is multiplexed with the traffic data.

**Publication No.** GB 2261349 B (Update 199439 E)

Publication Date: 19941019

Assignee: ERICSSON GE MOBILE COMMUNICATIONS (TELF)

Inventor: DENT P W

Language: EN

Application: WO 1991US5086 A 19910718 (PCT Application)

GB 199226465 A 19921218 (Local application)

Priority: US 1990556103 A 19900720

Related Publication: WO 1992002088 A (Based on OPI patent )

Original IPC: H04L-9/12(A)

Current IPC: H04L-9/00(R,A,I,M,JP,20060101,20051220,A,L) H04L-9/00(R,I,M,JP,20060101,20051220,C,L) H04L-9/12(R,I,M,EP,20060101,20051008,A) H04L-9/12(R,I,M,EP,20060101,20051008,C) H04W-12/00(R,I,M,EP,20090101,20090105,A) H04W-12/00(R,I,M,EP,20090101,20090105,C)

Current ECLA class: H04L-9/12 H04Q-7/38S H04W-12/02

Current ECLA ICO class: T04Q-7:38H

Claim: In a duplex communication system employing cryptographically encoded data within a digital cellular telecommunication network, a method which comprises: generating in a first base station within said network a first pseudo-random key stream of bits in accordance with an algorithm; combining in said first base station bits of said first key stream with a stream of data bits carrying communications information to be sent from said first base station to a mobile station to cryptographically encode said data stream and with a stream of cryptographically encoded data received from said mobile station to decode said data into communications information; generating in said mobile station a second pseudo-random key stream of bits in accordance with said algorithm; combining in said mobile station bits of said second key stream with a stream of data bits carrying communications information to be sent from said mobile station to said first base station to cryptographically encode said data stream and with a stream of cryptographically encoded data received from said first base station to decode said data into communications information; transmitting cryptographically encoded data on a high data rate message channel from said first base station to said mobile station and from said mobile station to said first base section; periodically transmitting synchronization information on a low data rate control channel from said first base station to said mobile station to synchronize said first and second key streams with one another; sending a command from said first base station to said mobile station indicative of a handoff of said mobile station to a second base station; generating in said second base station a third pseudo-random key stream of bits in accordance with said algorithm; transmitting for a selected period of time in response to said handoff command uncryptographically encoded synchronization information on a high data rate control channel from said second base station to said mobile station to synchronize said second and third key streams with one another; periodically transmitting synchronization information on a low data rate control channel from said second base station to said mobile station to synchronize said second and third key streams with one another; searching within said mobile station for synchronization information from said second base station on either said high data rate control channel or said low data rate control channel and, upon the detection of either, synchronizing said second pseudo-random key stream of said mobile station with said third pseudo-random keystream of said second base station; interrupting the transmission of uncryptographically encoded

synchronization information on said high data rate control channel from said second base station to said mobile station and beginning the transmission of cryptographically encoded data on a high data rate message channel in response to either the receipt by said second base station of correctly decodable cryptographically encoded data from said mobile station or the expiration of said selected period of time.

## **Japan**

**Publication No.** JP 6501139 W (Update 199410 E)

Publication Date: 19940203

Assignee: ERICSSON GE MOBILE COMMUNICATIONS (TELF)

Language: JA

Application: JP 1991516019 A 19910718 (Local application)

WO 1991US5086 A 19910718 (PCT Application)

Priority: US 1990556103 A 19900720

Related Publication: WO 1992002088 A (Based on OPI patent )

Original IPC: H04Q-7/04(A) H04B-7/26(B) H04L-9/00(B) H04L-9/10(B)

Current IPC: H04Q-7/04(A) H04B-7/26(B) H04L-9/00(B) H04L-9/10(B)

Current ECLA class: H04L-9/12 H04Q-7/38S H04W-12/02

Current ECLA ICO class: T04Q-7:38H

## **Korea**

**Publication No.** KR 123945 B1 (Update 199951 E)

Publication Date: 19971201

Assignee: ERICSSON GE MOBILE COMMUNICATIONS INC; US (TELF)

Language: KO

Application: WO 1991US5086 A 19910718 (PCT Application)

KR 1993700103 A 19930115 (Local application)

Priority: US 1990556103 A 19900720

Original IPC: H04L-9/02(A)

Current IPC: H04L-9/00(R,A,I,M,JP,20060101,20051220,A,L) H04L-

9/00(R,I,M,JP,20060101,20051220,C,L) H04L-9/12(R,I,M,EP,20060101,20051008,A) H04L-

9/12(R,I,M,EP,20060101,20051008,C) H04W-12/00(R,I,M,EP,20090101,20090105,A) H04W-

12/00(R,I,M,EP,20090101,20090105,C)

Current ECLA class: H04L-9/12 H04Q-7/38S H04W-12/02

Current ECLA ICO class: T04Q-7:38H

## **New Zealand**

**Publication No.** NZ 238652 A (Update 199426 E)

Publication Date: 19940325

Assignee: ERICSSON GE MOBILE COMMUNICATIONS (TELF)

Inventor: DENT P W

Language: EN

Application: NZ 238652 A 19910621 (Local application)

Priority: US 1990556103 A 19900720

Original IPC: H04L-9/16(A)

Current IPC: H04L-9/00(R,A,I,M,JP,20060101,20051220,A,L) H04L-

9/00(R,I,M,JP,20060101,20051220,C,L) H04L-9/12(R,I,M,EP,20060101,20051008,A) H04L-

9/12(R,I,M,EP,20060101,20051008,C) H04W-12/00(R,I,M,EP,20090101,20090105,A) H04W-

12/00(R,I,M,EP,20090101,20090105,C)

Current ECLA class: H04L-9/12 H04Q-7/38S H04W-12/02

Current ECLA ICO class: T04Q-7:38H

## United States

**Publication No.** US 5081679 A (Update 199206 B)

Publication Date: 19920114

### **Resynchronization of encryption systems upon handoff**

Assignee: Ericsson GE Mobile Communications Holding Inc. (TELF)

Inventor: Dent, Paul, SE

Agent: Johnson & Gibbs

Language: EN

Application: US 1990556103 A 19900720 (Local application)

Original IPC: H04L-9/02

Current IPC: H04L-9/00(R,I,M,JP,20060101,20051220,A,L) H04L-

9/00(R,I,M,JP,20060101,20051220,C,L) H04L-9/12(R,I,M,EP,20060101,20051008,A) H04L-

9/12(R,I,M,EP,20060101,20051008,C) H04W-12/00(R,I,M,EP,20090101,20090105,A) H04W-

12/00(R,I,M,EP,20090101,20090105,C)

Current ECLA class: H04L-9/12 H04Q-7/38S H04W-12/02

Current ECLA ICO class: T04Q-7:38H

Current US Class (main): 380-272000

Current US Class (secondary): 380-043000 380-260000 380-274000 455-438000

Original US Class (main): 38048

Original US Class (secondary): 37959 37960 38043 38049 45533.2

Original Abstract: A system for the synchronization of encryption and decryption in a duplex cellular radio system in which an encrypted call may be switched from one cell to another. At the instant of handoff, a rapid first resynchronization means temporarily seizes the voice channel in one direction only and transmits synchronization information in such one direction. The first resynchronization means ceases to transmit the synchronization information and releases such one direction of the voice channel as soon as an indicator of successful resynchronization is detected in the other direction.

Transmission of speech traffic in such one direction is then resumed after such detection of successful resynchronization. To avoid occupying such one direction with continuous transmission of the synchronization information in the event successful resynchronization has occurred but has not been detected due to faulty transmission in the other direction, an upper limit is set on the length of time which the first rapid synchronization means may cease such one direction. After such timeout, resynchronization information may be provided by a second resynchronization means at a slower rate through a slow rate control channel bit stream which is multiplexed with the traffic data.

Publication No. **WO 1992002088 A (Update 199208 E)**

**Publication Date: 19920206**

RESYNCHRONIZATION OF ENCRYPTION SYSTEMS UPON HANDOFF

**Assignee: ERICSSON GE MOBILE COMMUNICATIONS HOLDING INC., US**

**Inventor: DENT, PAUL, WILKINSON, SE**

**Language: EN**

**Application: WO 1991US5086 A 19910718 (Local application)**

**Priority: US 1990556103 A 19900720**

**Designated States: (National Original) AU CA GB JP KR**

**Original IPC: H04L-9/00**

**Current IPC: H04L-9/00(R,A,I,M,JP,20060101,20051220,A,L) H04L-9/00(R,I,M,JP,20060101,20051220,C,L) H04L-9/12(R,I,M,EP,20060101,20051008,A) H04L-9/12(R,I,M,EP,20060101,20051008,C) H04W-12/00(R,I,M,EP,20090101,20090105,A) H04W-12/00(R,I,M,EP,20090101,20090105,C)**

**Current ECLA class: H04L-9/12 H04Q-7/38S**

**Current ECLA ICO class: T04Q-7:38H**

**Original Abstract:** A system for the synchronization of encryption (203, 206) and decryption (204, 205) in a duplex cellular radio system in which an encrypted call (203, 206) may be switched from one cell to another. At the instant of handoff, a rapid first resynchronization means temporarily seizes the voice channel in one direction only and transmits synchronization information in such one direction. The first resynchronization means ceases to transmit the synchronization information and releases such one direction of the voice channel as soon as an indicator of successful resynchronization is detected in the other direction. Transmission of speech traffic in such one direction is then resumed after such detection of successful resynchronization. To avoid occupying such one direction with continuous transmission of the synchronization information in the event successful resynchronization has occurred but has not been detected due to faulty transmission in the other direction, an upper limit is set on the length of time which the first rapid synchronization means may cease such one direction. After such timeout, resynchronization information may be provided by a second resynchronization means at a slower rate through a slow rate control channel bit stream which is multiplexed (209 & 211) with the traffic data.

(19)日本国特許庁 (JP)

## (12) 公表特許公報 (A)

(11)特許出願公表番号

特表平6-501139

第7部門第3区分

(43)公表日 平成6年(1994)2月3日

(61)Int.Cl.<sup>5</sup> 認別記号 序内整理番号 F I  
 H 04 Q 7/04 K 7304-5K  
 H 04 B 7/26 108 A 7304-5K  
 H 04 L 9/00  
 9/10 7117-5K H 04 L 9/00 Z  
 審査請求 有 予審査請求 有 (全 22 頁) 最終頁に続く

(21)出願番号 特願平3-516019  
 (86) (22)出願日 平成3年(1991)7月18日  
 (85) 録件文提出日 平成5年(1993)1月19日  
 (86) 國際出願番号 PCT/US91/05086  
 (87) 國際公開番号 WO92/02088  
 (87) 國際公開日 平成4年(1992)2月6日  
 (31)優先権主張番号 556,108  
 (32)優先日 1990年7月20日  
 (33)優先権主張國 米国(US)  
 (81)指定国 AU, CA, GB, JP, KR

(71)出願人 エリクソン ジーイー モービル コミュニケーションズ インコーポレイテッド  
 アメリカ合衆国22709 ノース カロライナ州 リサーチ トライアングル パーク, トライアングル ドライブ 1, ピーク, オー, ボックス 13969  
 (72)発明者 デント, ポール, ウィルキンソン  
 スウェーデン固エスー 240 36 ステハグ, ステハグス プラストガード  
 (登録なし)  
 (74)代理人 井理士 浅村 雄 (外3名)

(54)【発明の名称】 ハンドオフ時における暗号化システムの再同期

## (57)【要約】

暗号化された通話(203、206)を1つのセルから別のものに切り換えることができる、二重セルラ無線システムにおける暗号化(203、206)と暗号解読(204、205)の同期のための方法。ハンドオフの場合、迅速第1再同期手段が、一方方向の音声チャンネルのみを中止し、このような一方的に同期情報を送信する。成功した再同期の指示が他方向において検出されるとすぐに、第1再同期手段は同期情報の送信を中止し、そして音声チャンネルのそのような一方を開放する。このような成功した再同期の検出後、そのような一方のスピーチトラフィックの送信が再開される。成功した再同期が行なわれたが他方向への送信不適によって検出されていない場合に、このような一方を同期情報の送信で占領してしまうことを回避するために、上階が、第1再同期手段がそのような一方を中止する時間長に設定される。このようなタイムアウトの後、再同期情報が、第2の再同期手段によって、より遅い速度で、トラフィックデータと多重化される(209及び211)低速制御チャンネルのビットストリームを通じて、与えられる。

